

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE
en sa qualité d'office élu

| | |
|---|--|
| Date d'expédition (jour/mois/année) 02 mai 2001 (02.05.01) | |
| Demande internationale no PCT/FR00/02024 | Référence du dossier du déposant ou du mandataire GEM 765 |
| Date du dépôt international (jour/mois/année) 12 juillet 2000 (12.07.00) | Date de priorité (jour/mois/année) 30 juillet 1999 (30.07.99) |
| Déposant CORON, Jean-Sébastien etc | |

1. L'office désigné est avisé de son élection qui a été faite:

☒ dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

26 février 2001 (26.02.01)

☐ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:2. L'élection ☒ a été faite☐ n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

| | |
|--|---|
| Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35 | Fonctionnaire autorisé Kiwa Mpay no de téléphone: (41-22) 338.83.38 |
|--|---|

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

| | | |
|---|---|---|
| Applicant's or agent's file reference GEM 765 | FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) | |
| International application No. PCT/FR00/02024 | International filing date (day/month/year) 12 July 2000 (12.07.00) | Priority date (day/month/year) 30 July 1999 (30.07.99) |
| International Patent Classification (IPC) or national classification and IPC H04L 9/32 | | |
| Applicant GEMPLUS | | |

| |
|--|
| <p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>8</u> sheets, including this cover sheet.</p> <p><input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of _____ sheets.</p> |
| <p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input checked="" type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input checked="" type="checkbox"/> Certain defects in the international application</p> <p>VIII <input checked="" type="checkbox"/> Certain observations on the international application</p> |

| | |
|---|--|
| Date of submission of the demand 26 February 2001 (26.02.01) | Date of completion of this report 05 November 2001 (05.11.2001) |
| Name and mailing address of the IPEA/EP | Authorized officer |
| Facsimile No. | Telephone No. |

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/02024

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages 1-21, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages 1-25, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR00/02024

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 3-6

because:

☐ the said international application, or the said claims Nos. _____
relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 3-6
are so unclear that no meaningful opinion could be formed (*specify*):

SEE SEPARATE SHEET

☐ the claims, or said claims Nos. _____ are so inadequately supported
by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. _____

2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:

☐ the written form has not been furnished or does not comply with the standard.

☐ the computer readable form has not been furnished or does not comply with the standard.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/02024

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III

Independent Claim 3 does not contain any technical feature defining the generation and verification of a signature. The expression "by appropriately selecting the data" has no limiting effect.

Independent Claim 4 does not contain any technical feature defining the generation and verification of a signature.

Claims 5 and 6 depend on Claim 3.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/02024

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|-------------------------------|--------|-----------|-----|
| Novelty (N) | Claims | 1-2, 7-25 | YES |
| | Claims | | NO |
| Inventive step (IS) | Claims | 1-2, 7-25 | YES |
| | Claims | | NO |
| Industrial applicability (IA) | Claims | 1-2, 7-25 | YES |
| | Claims | | NO |

2. Citations and explanations

The invention relates to electronic signature generation and verification methods based on the discrete logarithm problem, with total (Claims 1, 10, 13 and 16) or partial (Claims 2 and 8) message recovery.

The prior art:

The first document cited in the international search report describes such a method, with total message recovery, entitled the NYBERG-RUEPPEL signature scheme, Nyberg and Rueppel being the authors. The preambles to the independent claims are based on such a method.

The invention:

The methods of the invention have the aim of reducing the total size of the signature and message to be transmitted. Transmission is thereby quicker and a larger number of signatures can be stored when memory space is limited (for example, in a smart card).

No document from the international search report discloses or suggests the signature generation and verification steps defined in the characterising parts of independent

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/02024

Claims 1, 2, 8, 10, 13 and 16. Said claims meet the requirements of PCT Article 33.

Claims 7, 9, 11, 12, 14, 15 and 17-25 are dependent and, therefore, also meet, as such, the requirements of the PCT concerning novelty and inventive step.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/02024

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Contrary to the requirement of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in the article by NYBERG K. et al. entitled: "Message recovery for signature schemes based on the discrete logarithm problem", published in DESIGNS, CODES AND CRYPTOGRAPHY, JAN. 1996, KLUWER ACADEMIC PUBLISHERS, NETHERLANDS, vol. 7, no. 1-2, pages 61-8 has not been indicated in the description, nor has this document been cited.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR 00/02024

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Although Claims 1, 2, 8, 10, 13 and 16 have been written as separate independent claims, it appears that their scopes overlap or that they differ only by a variation in the definition of the subject matter for which protection is sought. Consequently, said claims are not **concise**. Moreover, taken as a whole, they are **unclear**, because the plurality of independent claims makes it difficult if not impossible to determine the subject matter for which protection is sought, and undue effort is required for a third party to determine the desired scope of protection.

Therefore, the claims taken as a whole do not meet the requirements of PCT Article 6.

2. Furthermore, taken individually, the following claims are unclear (PCT Article 6):
 - 2a. In Claim 1, line 17, the number f is not defined.
 - 2b. The term "improvement" used in dependent Claim 7 should have been deleted (PCT Guidelines, Chapter III-2.1) and the preamble to said claim should correspond to the same definition of the invention's aim as defined in independent Claim 2.
 - 2c. In independent Claim 8, the definition of the invention's aim ("method consisting in removing...") is unclear since the technical features of this claim relate to a signature generation and

VIII. Certain observations on the international application

verification method.

- 2d. The French text "*ledit procédé au schéma de signature*" in Claim 9 is unclear.
- 2e. The term "improvement" used in independent Claim 10 should have been deleted (PCT Guidelines, Chapter-III-2.1).
- 2f. The term "improvement" used in dependent Claim 11 should have been deleted (PCT Guidelines, Chapter-III-2.1).
- 2g. Claim 12 is written as a dependent claim but does not clearly indicate that it comprises all of the features of Claims 10 and 11. The following wording could be used, for example: A method according to Claims 10 and 11 which furthermore comprises the pre-processing step of...".
- 2h. The definition of the subject matter of independent Claim 13 is unclear. The term "improvement" should have been deleted and the additional features brought to the Nyberg-Rueppel method by said claim should have appeared in the characterising part.
- 2i. The term "improvement" used in dependent Claim 14 should have been deleted (PCT Guidelines, Chapter-III-2.1).
- 2j. Dependent Claim 15 refers to all of the preceding claims even though some of these do not relate to a signature scheme with partial message recovery

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 00/02024

VIII. Certain observations on the international application

(Claim 1, for example).

2k. The definition of the subject matter of independent Claim 16 is unclear. The term "improvement" should have been deleted and the additional features brought to the Nyberg-Rueppel method by said claim should have appeared in the characterising part.

21. Claims 20 to 25 are device claims (referring to a system) and not method claims like the "preceding" claims to which they refer. Furthermore, no passage in the description describes such devices. Therefore, device Claims 20 to 25 cannot be supported by the description, as required by PCT Article 6.

TRAITE DE COOPERATION EN MATIERE DE BREVETS


PCT

REC'D 07 NOV 2001

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

15 T

| | | | |
|--|---|--|--|
| Référence du dossier du déposant ou du mandataire GEM 765 PCT | | POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416) | |
| Demande internationale n° PCT/FR00/02024 | Date du dépôt international (jour/mois/année) 12/07/2000 | Date de priorité (jour/mois/année) 30/07/1999 | |
| Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/32 | | | |
| Déposant GEMPLUS et al. | | | |
| <p>1. Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.</p> <p>2. Ce RAPPORT comprend 8 feuilles, y compris la présente feuille de couverture.</p> <p><input type="checkbox"/> Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).</p> <p>Ces annexes comprennent feuilles.</p> | | | |
| <p>3. Le présent rapport contient des indications relatives aux points suivants:</p> <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Base du rapport II <input type="checkbox"/> Priorité III <input checked="" type="checkbox"/> Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle IV <input type="checkbox"/> Absence d'unité de l'invention V <input checked="" type="checkbox"/> Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration VI <input type="checkbox"/> Certains documents cités VII <input checked="" type="checkbox"/> Irrégularités dans la demande internationale VIII <input checked="" type="checkbox"/> Observations relatives à la demande internationale | | | |
| Date de présentation de la demande d'examen préliminaire internationale 26/02/2001 | | Date d'achèvement du présent rapport 05.11.2001 | |
| Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80293 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465 | | Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828 | |



RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02024

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-21 version initiale

Revendications, N°:

1-25 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
 - ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
 - ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).
3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
 - ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
 - ☐ remis ultérieurement à l'administration, sous forme écrite.
 - ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
 - ☐ La déclaration, selon laquelle le listage des séquences par-écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
 - ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.
4. Les modifications ont entraîné l'annulation :
- ☐ de la description, pages :
 - ☐ des revendications, - n°s :
 - ☐ des dessins, feuilles :

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR00/02024

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

III. Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

1. La question de savoir si l'objet de l'invention revendiquée semble être nouveau, impliquer une activité inventive (ne pas être évident) ou être susceptible d'application industrielle n'a pas été examinée pour ce qui concerne :

☐ l'ensemble de la demande internationale.

☒ les revendications n°s 3-6.

parce que :

☐ la demande internationale, ou les revendications n°s en question, se rapportent à l'objet suivant, à l'égard duquel l'administration chargée de l'examen préliminaire international n'est pas tenue effectuer un examen préliminaire international (*préciser*) :

☒ la description, les revendications ou les dessins (*en indiquer les éléments ci-dessous*), ou les revendications n°s 3-6 en question ne sont pas clairs, de sorte qu'il n'est pas possible de formuler une opinion valable (*préciser*) :
voir feuille séparée

☐ les revendications, ou les revendications n°s en question, ne se fondent pas de façon adéquate sur la description, de sorte qu'il n'est pas possible de formuler une opinion valable.

☐ il n'a pas été établi de rapport de recherche internationale pour les revendications n°s en question.

2. Le listage des séquences de nucléotides ou d'acides aminés n'est pas conforme à la norme prévue dans l'annexe C des instructions administratives, de sorte qu'il n'est pas possible d'effectuer un examen préliminaire international significatif:

☐ le listage présenté par écrit n'a pas été fourni ou n'est pas conforme à la norme.

☐ le listage sous forme déchiffrable par ordinateur n'a pas été fourni ou n'est pas conforme à la norme.

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

**RAPPORT D'EXAMEN
PRÉLIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR00/02024

| | | |
|--|----------------------|-----------|
| Nouveauté | Oui : Revendications | 1-2, 7-25 |
| | Non : Revendications | |
| Activité inventive | Oui : Revendications | 1-2, 7-25 |
| | Non : Revendications | |
| Possibilité d'application industrielle | Oui : Revendications | 1-2, 7-25 |
| | Non : Revendications | |

2. Citations et explications
voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

Concernant le point III

Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

La revendication indépendante 3 ne contient aucune caractéristique technique définissant la génération et la vérification d'une signature. L'expression "en choisissant convenablement les données" n'est pas limitative.

La revendication indépendante 4 ne contient aucune caractéristique technique définissant la génération et la vérification d'une signature.

Les revendications 5 et 6 sont dépendantes de la revendication 3.

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'invention concerne des procédés de génération et vérification de signature électronique basés sur le problème du logarithme discret, avec reconstitution totale (revendications 1, 10, 13 et 16) ou partielle du message (revendications 2 et 8).

Etat de la technique:

La première citation du rapport de recherche internationale décrit un tel procédé, avec reconstitution totale du message, appelé schéma de signature de NYBERG ET RUEPPEL, du nom des auteurs. Les préambules des revendications indépendantes sont basés sur un tel procédé.

Invention:

Les procédés selon l'invention ont pour but de réduire la taille totale de la signature et du message à transmettre. La transmission est ainsi plus rapide et, lorsque la place

en mémoire est limitée (par ex. carte à puce) il est possible de stocker un plus grand nombre de signatures.

Aucun document du rapport de recherche internationale ne divulgue ou suggère les étapes de génération et de vérification de signature définies dans les parties caractérisantes des revendications indépendantes 1, 2, 8, 10, 13 et 16. Ces revendications remplissent les conditions de l'article 33 PCT.

Les revendications 7, 9, 11, 12, 14, 15, 17- 25 sont dépendantes et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

Concernant le point VII

Irrégularités dans la demande internationale

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans l'article de NYBERG K. et al. intitulé: "Message recovery for signature schemes based on the discrete logarithm problem", publié dans DESIGNS, CODES AND CRYPTOGRAPHY, JAN. 1996, KLUWER ACADEMIC PUBLISHERS, NETHERLANDS, vol. 7, no. 1-2, pages 61-8, et ne cite pas ce document.

Concernant le point VIII

Observations relatives à la demande internationale

1. Bien que les revendications 1, 2, 8, 10, 13 et 16 aient été rédigées sous forme de revendications indépendantes distinctes, il semble qu'elles aient des portées se recoupant ou qu'elles ne diffèrent l'une de l'autre que par une variation dans la définition de l'objet pour lequel la protection est demandée. Par conséquent ces revendications ne sont pas **concises**. De plus, prises dans leur ensemble, elles sont dénuées de **clarté**, car du fait de la pluralité des revendications indépendantes, il est difficile, voire impossible de déterminer l'objet pour lequel une protection est demandée, et la délimitation par un tiers de l'étendue de la

protection demandée nécessite des efforts excessifs.

Par conséquent, les revendications prises dans leur ensemble ne satisfont pas aux conditions requises à l'article 6 PCT.

2. De plus, prises individuellement, les revendications suivantes ne sont pas claires (Article 6 PCT):
 - 2a. Dans la revendication 1, à la ligne 17, le nombre f n'est pas défini.
 - 2b. Le terme "amélioration" dans la revendication dépendante 7 aurait dû être supprimé (Directives PCT, III-2.1) et le préambule de cette revendication devrait correspondre à la même définition de l'objet de l'invention que celui défini dans la revendication indépendante 2.
 - 2c. Dans la revendication indépendante 8, la définition de l'objet de l'invention ("procédé consistant à enlever...") n'est pas claire car les caractéristiques techniques de cette revendication se rapportent à un procédé de génération et de vérification de signature.
 - 2d. L'expression "ledit procédé au schéma de signature" dans la revendication 9 n'est pas claire.
 - 2e. Le terme "amélioration" dans la revendication indépendante 10 aurait dû être supprimé (Directives PCT, III-2.1).
 - 2f. Le terme "amélioration" dans la revendication dépendante 11 aurait dû être supprimé (Directives PCT, III-2.1).
 - 2g. La revendication 12 est formulée comme une revendication dépendante mais n'indique pas clairement qu'elle comporte toutes les caractéristiques de revendications 10 et 11, par exemple avec une formulation du type: Procédé selon les revendications 10 et 11, comportant de plus l'étape de prétraitement consistant à..."

- 2h. La définition de l'objet de la revendication indépendante 13 n'est pas claire: le terme "amélioration" aurait dû être supprimé et les caractéristiques supplémentaires que la revendication apporte au procédé de Nyberg et Rueppel placées dans la partie caractérisante.
- 2i. Le terme "amélioration" dans la revendication dépendante 14 aurait dû être supprimé (Directives PCT, III-2.1).
- 2j. La revendication dépendante 15 se réfère à toutes les revendications précédentes bien que certaines ne concerne pas un schéma de signature avec reconstitution partielle de message (par exemple la revendication 1).
- 2k. La définition de l'objet de la revendication indépendante 16 n'est pas claire: le terme "amélioration" aurait dû être supprimé et les caractéristiques supplémentaires que la revendication apporte au procédé de Nyberg et Rueppel placées dans la partie caractérisante.
- 2l. Les revendications 20 à 25 sont des revendications de dispositif (système) et non de procédé (méthode) comme les revendications "précédentes" auxquelles elles se réfèrent. De plus aucun passage de la description ne décrit de tels dispositifs. Les revendications 20 à 25 de dispositifs ne peuvent donc pas se fonder sur la description, comme l'exige l'article 6 PCT.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

| | | |
|---|---|--|
| Référence du dossier du déposant ou du mandataire GEM 765 | POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après | |
| Demande internationale n° PCT/FR 00/ 02024 | Date du dépôt international(jour/mois/année) 12/07/2000 | (Date de priorité (la plus ancienne) (jour/mois/année) 30/07/1999 |
| Déposant GEMPLUS | | |

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

☐ contenu dans la demande internationale, sous forme écrite.

☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

☐ remis ultérieurement à l'administration, sous forme écrite.

☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,

☒ le texte est approuvé tel qu'il a été remis par le déposant.

☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

☒ le texte est approuvé tel qu'il a été remis par le déposant

☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

☐ suggérée par le déposant.

☐ parce que le déposant n'a pas suggéré de figure.

☐ parce que cette figure caractérise mieux l'invention.

☒ Aucune des figures n'est à publier.

| A. CLASSEMENT DE L'OBJET DE LA DEMANDE CIB 7 H04L9/32 | | |
|---|---|--|
| Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB | | |
| B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE | | |
| Documentation minimale consultée (système de classification suivi des symboles de classement) CIB 7 H04L | | |
| Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche | | |
| Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés) INSPEC, WPI Data, PAJ | | |
| C. DOCUMENTS CONSIDERES COMME PERTINENTS | | |
| Catégorie ° | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
| A | NYBERG K ET AL: "Message recovery for signature schemes based on the discrete logarithm problem" DESIGNS, CODES AND CRYPTOGRAPHY, JAN. 1996, KLUWER ACADEMIC PUBLISHERS, NETHERLANDS, vol. 7, no. 1-2, pages 61-81, XP000905401 ISSN: 0925-1022 page 67 -page 72 --- | 1-25 |
| A | EP 0 639 907 A (R3 SECURITY ENGINEERING AG) 22 février 1995 (1995-02-22) colonne 3, ligne 43 -colonne 9, ligne 4 --- -/-- | 1-25 |
| <input checked="" type="checkbox"/> Voir la suite du cadre C pour la fin de la liste des documents <input checked="" type="checkbox"/> Les documents de familles de brevets sont indiqués en annexe | | |
| ° Catégories spéciales de documents cités: "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent "E" document antérieur, mais publié à la date de dépôt international ou après cette date "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée) "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée "T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention "X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier "&" document qui fait partie de la même famille de brevets | | |
| Date à laquelle la recherche internationale a été effectivement achevée 15 septembre 2000 | | Date d'expédition du présent rapport de recherche internationale 21/09/2000 |
| Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016 | | Fonctionnaire autorisé Zucka, G |

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|-----------|--|-------------------------------|
| A | <p>KAISA NYBERG & RAINER A. RUEPPEL: "A new signature scheme based on the DSA giving message recovery"</p> <p>PROCEEDINGS OF THE 1ST ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY,</p> <p>3 - 5 mai 1993, pages 58-61, XP000908795</p> <p>Fairfax, VA USA</p> <p>cité dans la demande</p> <p>page 58 -page 59</p> <p>-----</p> | 1-25 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 00/02024

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---------------------|----------------------------|---------------------|
| EP 0639907 A | 22-02-1995 | AT 187588 T | 15-12-1999 |
| | | CA 2130250 A | 18-02-1995 |
| | | DE 69327238 D | 13-01-2000 |
| | | DE 69327238 T | 07-09-2000 |
| | | US 5600725 A | 04-02-1997 |
| ----- | | | |